Licence 2 - 2020/2021

HLMA304 : Arithmétique

Thierry Mignon

Octobre 2020

Correction du contrôle continu

Durée : 1h30 – Documents, calculatrices et téléphones interdits

Exercice 1. *Cours.* Soit (a, b) un couple d'entiers ; énoncer et démontrer le résultat d'existence et d'unicité de la division euclidienne de a par b.

> CORRECTION : *cf.* cours.

Exercice 2. Prouver que, pour tout entier relatif m, la fraction

$$\frac{21m+4}{14m+3}$$

est irréductible.

> CORRECTION : Il s'agit de prouver que, pour tout entier relatif m, $21m+4$ et $14m+3$ sont premiers entre eux.
> Soit $m \in \mathbb{Z}$. On a vu en cours que, si a, b, c, d sont quatre entiers tels que $a = bc + d$, alors $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, d)$. On constate, par exemple en effectuant la division euclidienne *polynomiale* du polynôme en m "$21m+4$" par le polynôme en m "$14m+3$", que :
>
> $$(21m+4) = 1.(14m+3) + (7m+1),$$
>
> donc $\mathrm{pgcd}(21m+4, 14m+3) = \mathrm{pgcd}(14m+3, 7m+1)$. On observe ensuite que :
>
> $$(14m+3) = 2.(7m+1) + (1),$$
>
> donc $\mathrm{pgcd}(14m+3, 7m+1) = \mathrm{pgcd}(7m+1, 1) = 1$.

Exercice 3. Soit $P = (x, y)$ un point du plan $\mathbb{R}^2$. On dira que P est *entier* si l'abscisse x et l'ordonnée y de P sont tous deux dans $\mathbb{Z}$.

(1) Trouver l'ensemble des points entiers de la droite :

$$345x + 714y - 6 = 0$$

Correction : Calculons d'abord pgcd$(345, 714)$ à l'aide de l'algorithme d'Euclide :

$$714 = 2 \times 345 + 24, \quad 345 = 14 \times 24 + 9, \quad 24 = 2 \times 9 + 6, \quad 9 = 1 \times 6 + 3, \quad 6 = 2 \times 3 + 0$$

donc $714 \wedge 345 = 3$. Puisque 3 divise le second membre de l'équation, on sait qu'elle possède une infinité de solutions. Elle est de plus équivalente à l'équation obtenue en divisant tout par 3 :

$$115x + 238y = 2 \qquad (\star)$$

Cherchons une solution particulière de $(\star)$ en calculant des coefficients de Bezout pour 115 et 238. On utilise pour cela l'algorithme d'Euclide augmenté :

$$238 = 2 \times 115 + 8, \quad 115 = 14 \times 8 + 3, \quad 8 = 2 \times 3 + 2, \quad 3 = 1 \times 2 + 1$$

puis, en remontant les équations :

$$\begin{aligned} 1 &= 3 - 2 = 3 - (8 - 2 \times 3) = -8 + 3 \times 3 = -8 + 3 \times (115 - 14 \times 8) \\ &= 3 \times 115 - 43 \times 8 = 3 \times 115 - 43 \times (238 - 2 \times 115) = 89 \times 115 - 43 \times 238 \end{aligned}$$

En multipliant cette égalité par 2 on obtient :

$$115 \times 178 + 238 \times (-86) = 2$$

Le couple $(x_0, y_0) = (178, -86)$ est donc une solution particulière de l'équation $(\star)$.
Soit maintenant $(x, y) \in \mathbb{Z}^2$ une solution quelconque. La différence des deux égalité : $115x+238y = 2$ et $115x_0+238y_0 = 2$ nous donne : $115(x-x_0) = -238(y-y_0)$, et l'entier 115 divise $-238(y-y_0)$. D'après le lemme de Gauss, applicable ici puisque $115 \wedge 238 = 1$, 115 divise $(y - y_0)$ et il existe $k \in \mathbb{Z}$ tel que $y = y_0 + 115k$. En remplaçant $(y - y_0)$ par $115k$ dans l'égalité ci-dessus on obtient ensuite : $x = x_0 - 238k$. On vérifie aisément que tous les couples $(x_0 - 238k, y_0 + 115k)$ sont bien des solutions.
L'ensemble des solutions est donc :

$$\{(178 - 238k, -86 + 115k), \; k \in \mathbb{Z}\}$$

(2) Soit D une droite d'équation :

$$ax + by + c = 0, \qquad \text{où } (a, b, c) \in \mathbb{Z}^3.$$

Montrer que D contient soit aucun, soit une infinité de points entiers. Donner des exemples de chacune des deux situations.

Correction : Supposons que l'équation possède *au moins* une solution (x_0, y_0), on constate que tous les couples $(x_0 - kb, y_0 + ka)$, où $k \in \mathbb{Z}$, sont aussi des solutions. Il y a donc une infinité de solutions.
Montrons que ces deux cas (ensemble de solution vide et ensemble de solutions infini) sont possibles :
Exemple 1 : $2x + 2y = 1$. Le terme de gauche est toujours pair et ne peut valoir 1. Plus généralement, dès que $a \wedge b$ ne divise pas c, il n'y a pas de solution.
Exemple 2 : $x + y = 0$. Tous les couples $(k, -k)$ sont solutions. Plus généralement, dès que $a \wedge b$ divise c, il y a une infinité de solutions.

Exercice 4. Trouver tous les couples $(a,b) \in \mathbb{N}^2$ tels que $a \wedge b = 30$ et $a \vee b = 600$.

CORRECTION : Écrivons $a = 30a', b = 30b'$ où $a', b' \in \mathbb{Z}$. On sait que $a' \wedge b' = 1$. Le produit du pgcd et du ppcm vaut ab et l'on a :

$$a \vee b \times a \wedge b = ab \iff 30.600 = ab = 30a'.30b' \iff 20 = a'b'$$

Il nous suffit donc de trouver tous les couples $(a', b') \in \mathbb{N}^2$ tels que $a' \wedge b' = 1$ et $a'b' = 20$. On procède en listant les diviseurs de 20 :
- Si $a' = 1$, $b' = 20$, on obtient la solution $(a,b) = (30, 600)$.
- Si $a' = 2$, $b' = 10$, impossible car ils ne sont pas premiers entre eux.
- Si $a' = 4$, $b' = 5$, on obtient la solution $(a,b) = (120, 150)$.
- Si $a' = 5$, $b' = 4$, on obtient la solution $(a,b) = (150, 120)$.
- Si $a' = 10$, $b' = 2$, impossible car ils ne sont pas premiers entre eux.
- Si $a' = 20$, $b' = 1$, on obtient la solution $(a,b) = (600, 30)$.

L'ensemble des solution est donc : $\{(30, 600), (120, 150), (150, 120), (600, 30)\}$.

Exercice 5. On rappelle que la valuation 2-adique d'un nombre entier n est le plus grand entier naturel k tel que 2^k divise n. Dit autrement, c'est l'exposant du nombre premier 2 dans la décomposition en facteurs premiers de n. On la note $v_2(n)$.

(1) Calculer les valuations 2-adiques de $5+1$, 5^2+1. Calculer ensuite celles de $5-1$, 5^2-1.

CORRECTION :
- $5 + 1 = 6 = 2^1.3^1$, donc $v_2(5+1) = 1$.
- $5^2 + 1 = 26 = 2^1.13^1$, donc $v_2(5^2+1) = 1$.
- $5 - 1 = 4 = 2^2$, donc $v_2(5-1) = 2$.
- $5^2 - 1 = 24 = 2^3.3$, donc $v_2(5^2-1) = 3$.

(2) Montrer que, quelque soit k dans $\mathbb{N}^*$, $5^k + 1$ n'est pas divisible par 4. En déduire $v_2(5^k+1)$ pour $k \in \mathbb{N}^*$.

CORRECTION : On sait que $5 \equiv 1[4]$, donc $5^k \equiv 1[4]$ et $5^k + 1 \equiv 2[4]$ n'est pas congru à 0 modulo 4. (On pouvait aussi procéder par récurrence, un peu comme dans la question suivante.)
Puisque $k \geq 1$, $5^k + 1$ est pair. Donc $2|(5^k+1)$ mais $2^2 \not| (5^k+1)$. Ceci montre que $v_2(5^k+1) = 1$.

(3) Calculer, par récurrence sur $n \in \mathbb{N}$, la valuation 2-adique de $5^{(2^n)} - 1$.

Correction : Les exemples de la question (1) nous amènent à poser pour tout entier $n \in \mathbb{N}$ l'hypothèse de récurrence

$$H_n \ : \quad v_2(5^{2^n} - 1) = n + 2$$

Si $n = 0$ ou $n = 1$, H_n est vrai d'après la question (1).
Supposons H_n vraie. Montrons H_{n+1}.
On observe que :

$$5^{2^{n+1}} + 1 = \left(5^{2^n}\right)^2 - 1 = (5^{2^n} - 1)(5^{2^n} + 1).$$

D'après la question précédente $v_2(5^{2^n} + 1) = 1$. D'après l'hypothèse de récurrence $v_2(5^{2^n} - 1) = n+2$. Les exposants de 2 s'additionnent dans les produits des décompositions en facteurs premiers, donc $v_2(5^{2^{n+1}} - 1) = (n + 2) + 1 = n + 3$.